P3NK-4472-08Z0

FUJITSU Network Si-R
Si-R Gシリーズ

トラブルシューティング V2

FUJITSU

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットやLANをさらに活用するために、本装置をご利用ください。

2011年11月初版
2012年 3月第2版
2012年 8月第3版
2013年 1月第4版
2013年 3月第5版
2013年 6月第6版
2014年 1月第7版
2014年11月第8版

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。
従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。
Microsoft Corporationのガイドラインに従って画面写真を使用しています。
Copyright FUJITSU LIMITED 2011 - 2014

目次

はじめに 2
本書の使いかた 4
本書の読者と前提知識 4
本書における商標の表記について 5
本装置のマニュアルの構成 6
1 回線料金がおかしいと思ったら 7
1.1 超過課金の見分け方 7
1.2 超過課金が発生した原因を調べる 7
2 通信ができない場合には 11
2.1 起動時の動作に関するトラブル 11
2.2 本装置設定時のトラブル 12
2.3 回線への接続に関するトラブル 14
2.4 データ通信に関するトラブル 15
2.5 導入に関するトラブル 17
2.6 IPsec/IKE に関するトラブル 18
2.7 認証機能に関するトラブル 34
2.8 SNMP に関するトラブル 36
2.9 VRRP に関するトラブル 37
2.10 外部メディアスタート機能に関するトラブル 41
2.11 その他のトラブル 41
3 コマンド入力が正しくできないときには 42
3.1 シェルに関するトラブル 42
4 ソフトウェア更新に失敗したときには（バックアップファーム機能） 43
4.1 パソコン（FTP クライアント）を準備する 43
4.2 本装置を準備する 43
4.3 ソフトウェアを更新する 44
5 ご購入時の状態に戻すには 45
5.1 LAN で接続する 45
5.2 コンソールポートに接続する 47
5.3 SELECT ボタン／ ENTER ボタンを使用する 49
索引 50

本書の使いかた

本書では、困ったときの原因・対処方法やご購入時の状態に戻す方法について説明しています。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

ヒント	**本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。**
こんな事に気をつけて	**本装置をご使用になる際に、注意していただきたいことを説明しています。**
	操作手順で説明しているもののほかに、補足情報を説明しています。
	操作方法など関連事項を説明している箇所を示します。
	本装置の機能を使用する際に、対象となる機種名を示します。
	製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。
	製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

本書における商標の表記について

Microsoft、Windows、Windows NT、Windows ServerおよびWindows Vistaは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

Adobeおよび Readerは、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における商標または登録商標です。

UNIXは、米国およびその他の国におけるオープン・グループの登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

製品名称	本文中の表記
Microsoft® Windows® XP Professional operating system	Windows XP
Microsoft® Windows® XP Home Edition operating system	
Microsoft® Windows® 2000 Server Network operating system	Windows 2000
Microsoft® Windows® 2000 Professional operating system	
Microsoft® Windows NT® Server network operating system Version 4.0	Windows NT 4.0
Microsoft® Windows NT® Workstation operating system Version 4.0	
Microsoft® Windows Server® 2003, Standard Edition	Windows Server 2003
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise Edition	
Microsoft® Windows Server® 2003 R2, Enterprise Edition	
Microsoft® Windows Server® 2003, Datacenter Edition	
Microsoft® Windows Server® 2003 R2, Datacenter Edition	
Microsoft® Windows Server® 2003, Web Edition	
Microsoft® Windows Server® 2003, Standard x64 Edition	
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise x64 Edition	
Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition	
Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based systems	
Microsoft® Windows Server® 2003, Datacenter x64 Edition	
Microsoft® Windows Server® 2003 R2, Datacenter x64 Edition	
Microsoft® Windows Vista® Ultimate operating system	Windows Vista
Microsoft® Windows Vista® Business operating system	
Microsoft® Windows Vista® Home Premium operating system	
Microsoft® Windows Vista® Home Basic operating system	
Microsoft® Windows Vista® Enterprise operating system	
Microsoft® Windows® 7 64bit Home Premium	Windows 7
Microsoft® Windows® 7 32bit Professional	

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
Si-R効率化運用ツール使用手引書	Si-R効率化運用ツールを使用する方法を説明しています。
Si-R G100　ご利用にあたって	Si-R G100の設置方法やソフトウェアのインストール方法を説明しています。
Si-R G200　ご利用にあたって	Si-R G200の設置方法やソフトウェアのインストール方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング（本書）	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様とMIB/Trap一覧を説明しています。
コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
コマンド設定事例集	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
コマンドリファレンス -構成定義編-	構成定義コマンドの項目やパラメタの詳細な情報を説明しています。
コマンドリファレンス -運用管理編-	運用管理コマンド、その他のコマンドの項目やパラメタの詳細な情報を説明しています。
Webユーザーズガイド	Web画面を使用して、基本的な操作やメンテナンスについて説明しています。 また、Web画面の項目の詳細な情報を説明しています。

1 回線料金がおかしいと思ったら

超過課金とは、利用者が意図しない回線接続や回線使用が長期的に続き、その結果として必要以上の回線料金が課金されることがあります。

以下に超過課金の見分け方と調査方法などについて説明します。

1.1 超過課金の見分け方

超過課金が発生する原因は2つあります。

（1） 回線未接続状態でLANに接続したパソコンなどから利用者の意図しないデータが回線に流れ、その結果、回線が接続することが頻発する場合。

（2） 回線を接続したあとに、LANに接続されたパソコンなどから利用者の意図しないデータが定期的に発信され、回線が長時間接続されたままの状態になる場合。

これらは課金情報を確認し、利用状況と照らし合わせることで超過課金が発生していることがわかります。課金情報で表示されている回線接続していた時間が利用時間よりも極端に長い場合は、超過課金が発生している可能性があります。

1.2 超過課金が発生した原因を調べる

ここでは、超過課金が発生する代表的な事例をあげ、それぞれの調査方法と対処方法について説明します。

WAN側にRIPパケットが流れている場合

【現象】 LAN側のパソコンの通信が終了したが、長時間回線が自動切断されない。

【原因】 WAN側接続相手（たとえばプロバイダのルータ）がダイナミックルーティングを使用し、本装置に経路情報（RIPパケット）を送信してくる場合に、通信がないにもかかわらず回線が接続されたままになることがあります。

【調査方法】

- まずLAN側端末が回線を使用した通信を行っていないことを確認します。
- もし、パソコンが通信しているかが判断できない場合は、それらのパソコンの電源を切断します。
- この状態で本装置の表示ランプを監視します。ここでB1またはB2ランプが一定間隔（15～45秒間隔）で点滅していた場合は、経路情報などのなんらかのデータが接続相手から送られてきていることになります。
- さらに上記ランプが点滅するたびにIP統計情報を確認します。表示されたIP統計情報の中のudp XXX datagrams receivedの部分の数字が確認するたびに増加していれば、原因は経路情報（RIP）受信によるものと考えられます。

【対処】 IPフィルタリング機能を使って経路情報（RIP）を破棄するように以下の設定をしてください。

```
remote <number> ip filter <count> reject any any any any 520 17 yes any any
```

これにより、接続相手から経路情報（RIP）が送出されてきても無通信監視時間（初期設定値は60秒）を経過すると回線は自動的に切断されます。

補足 上記以外にも本装置の設定でWAN側にダイナミックルーティング機能を使用する設定になっていることが原因の場合もあります。この場合は、以下のコマンドでRIP送信をしない設定であることを確認してください。

```
# show running-config remote <number> ip rip
```

参照 コマンド設定事例集「2.12 IPフィルタリング機能を使う」（P.128）

パソコンからの自動送信パケット

【現象】 LAN側のパソコンなどからの通信がないにもかかわらず、いつのまにか本装置からの発信により回線接続してしまう。

【原因】 Windowsのパソコンは、利用者の意図とは無関係に（利用者が通信している意識がないにもかかわらず）自動的にパケットを回線側に送出してしまう場合があります。

【調査方法】

- 利用者が通信していないこと（WWWブラウザや電子メールなど使用していないこと）を確認してください。
- この状態で回線の発信が起きている場合は、システムログ（メッセージ集）を参照して発信の契機となった事象を確認してください。
- 発信ログの意味が「パケット送信による発信処理」の場合は、パソコンが回線側にパケットを送信しています。→【対処1】
- 発信ログの意味が「上記以外の理由による発信処理」の場合で、発信理由がProxyDNSの場合は、パソコンが本装置のProxyDNS機能を利用しようとしてDNS要求を送信しています。→【対処2】

【対処1】IPフィルタリング機能を使ってNetBIOS over TCPの情報を回線側に流さないように設定してください。

参照 コマンド設定事例集「2.12 IPフィルタリング機能を使う」（P.128）

【対処2】URLフィルタ機能を使ってWindowsのワークグループ名のアクセスを禁止してください。この場合はアクセスを禁止するドメイン名に「＜ワークグループ名＞＊」を指定してください。

参照 コマンド設定事例集「2.24 特定のURLへのアクセスを禁止する（URLフィルタ機能）」（P.379）

【対処3】パソコンが送信するDNSパケットの問い合わせタイプ（QTYPE）がA（1）、PTR（12）以外の場合、DNS問い合わせタイプフィルタ機能を使って、特定の問い合わせタイプのパケットを破棄することができます。DNSパケットの問い合わせタイプ（QTYPE）は、本装置のシステムログ情報に以下の情報が記録されていることから確認してください。
「proxydns:[<QTYPE>:<QNAME>]from<IPアドレス>to<ネットワーク名>」

参照 コマンド設定事例集「2.23.5 DNS問い合わせタイプフィルタ機能を使う」（P.377）

デフォルトルートどうしで接続している場合

【現象】 パソコン上のアプリケーション（WWW ブラウザや電子メールなど）が異常終了し、数分から数十分間回線が接続されたままになる。

【原因】 自側および相手側本装置の両方でデフォルトルートの設定がされていることが原因です。

【調査方法】

両者のデフォルトルートの設定内容を確認してください。

【対処】 どちらかの本装置の設定からデフォルトルートの設定を外してください。

スケジュール機能の設定を誤った場合

【現象】 スケジュール機能で夜間は発信抑止しているにもかかわらず、発信してしまう。

【原因】 スケジュール機能の設定が誤っていることが原因です。

【調査方法】

- スケジュール機能の設定を確認してください。ここで予約時刻、終了時刻が正しく設定されているかを確認してください。
- さらに内部時刻の時刻設定も確認してください。

【対処】 上記スケジュール機能および内部時刻の時刻設定をそれぞれ正しく設定し直してください。

☛ 参照 コマンド設定事例集「2.31 スケジュール機能を使う」（P.406）、
コマンドユーザーズガイド「1.2 時刻を設定する」（P.13）

LAN 側のパソコンを移設した場合

【現象】 ほかの LAN に接続してあったパソコンなどを本装置の LAN に移設したら、頻繁に回線発信が行われるようになった。または回線が切断されなくなった。

【原因】 そのパソコンが以前接続していた LAN 環境で運用されていたサービスやアプリケーションが WAN 環境にはふさわしくないことが原因です。

【調査方法】

問題のパソコンが立ち上がっているときと電源が切断されているときとで、上記現象の発生の有無が変わることを確認してください。

【対処】 詳細な原因は、問題となるサービスやアプリケーションに依存するため対応方法はさまざまです。特定のサーバや特定のサービスへのアクセスが原因の場合、IP フィルタリング機能を使用して無意味な発信を抑止します。また、スケジューリング機能を使用することで防止できる場合もあります。どの場合にもシステムログ情報を確認して発信の契機となったサービスやアプリケーションを特定するか、またはそのパソコンの以前の利用者にサービス内容やアプリケーションの設定内容を確認してください。

本装置を移設した場合

【現象】　ほかの環境に接続していた本装置を移設した、本装置が関係するネットワークの一部または全部が変更になったところ、回線発信が頻発するようになった。または回線が切断されなくなった。

【原因】　本装置の設定が新たな環境にふさわしくないものであることが原因です。

【調査方法】

特に必要ありません。

【対処】　本装置の設定を一度ご購入時の状態に戻したあと、最初から設定し直してください。

参照 「5 ご購入時の状態に戻すには」（P.45）

2　通信ができない場合には

通信ができない場合、さまざまな原因が考えられます。まず、以下を参考に本装置の動作状況を確認してみてください。

ヒント

◆ エラー番号からトラブルの原因を探る

エラーログ情報に表示されたエラー番号から、エラーの原因をある程度特定できます。

エラーログ情報をプリントアウトして保管しておくことをお勧めします。

⚠警告

• 決してご自身では修理を行わないでください。

• 本装置が故障した場合は、弊社の技術者または弊社が認定した技術員によるメンテナンスを受けてください。

2.1　起動時の動作に関するトラブル

本装置起動時のトラブルには、以下のようなものがあります。

- **POWER ランプがつかない**

【原因】　電源ケーブルが、電源コネクタまたはコンセントに正しく接続されていません。

【対処】　電源ケーブルを、電源コネクタまたはコンセントに正しく接続してください。

【原因】　本装置の電源スイッチが入っていません。

【対処】　本装置の電源スイッチが「｜」側へ押されているか確認してください。

- **CHECK ランプが橙色で点灯している**

【原因】　本装置に異常が発生しました。

【対処】　弊社の技術員または弊社が認定した技術員へ連絡してください。

- **CHECK ランプが橙色で点灯している**
  接続したポートに該当する通信状態を示すランプが点灯していない
  show system status 実行時の machine_state が、“FALLBACK” となっている

【原因】　ハード障害を検出したため、縮退モードに遷移しました。

【対処】　弊社の技術員または弊社が認定した技術員へ連絡してください。

2.2 本装置設定時のトラブル

本装置設定時のトラブルには、以下のようなものがあります。

● 接続したETHERNETポートのランプが点灯していない、または、パソコンまたはHUBのリンクランプが点灯していない

【原因】 スピード／全二重・半二重のモード設定が接続相手と合っていません。

【対処】 本装置の10／100／1000Mおよび FULL／HALFの設定とパソコンまたはHUBの接続状態が合っているか確認してください。本装置はLINK／ACT／SPEEDランプ、FDXランプまたはステータスコマンド（show ether）で接続状態が確認できます。

☛参照 Si-R G200　ご利用にあたって「ランプの詳細」（P.20）
Si-R G100　ご利用にあたって「ランプの詳細」（P.20）

【原因】 LANケーブルのタイプが違います。

【対処】 LAN機器と接続する場合、パソコンにはストレートケーブル、HUBにはクロスケーブルで接続する必要があります。ケーブルのタイプを確認して、必要なLANケーブルを用意してください。

【原因】 接続に誤りがあります。または、LANケーブルが断線しています。

【対処】 点灯していない場合は、LANケーブルが正しく接続されていないか、または断線している可能性があります。LANケーブルがパソコンまたはHUBと本装置に正しく差し込んであるかを確認し、それでも点灯しない場合は、別のLANケーブルに交換してください。

【原因】 ETHERNETポートのAutoMDI/MDI-Xの設定がonの状態で、ETHERNETポートに接続しているパソコンまたはHUBのETHERNETポートがAutoMDI/MDI-Xとなっている場合に、正常に接続できていません。

【対処】 本装置のETHERNETポートのAutoMDI/MDI-Xの設定をoffにします。または、ETHERNETポートに接続しているパソコンまたはHUBのETHERNETポートの設定をoffにします。

● POWER／CHECKランプ以外のランプが点灯していない

【原因】 運用中に本装置のランプを消灯する設定になっているか、または、ECOモードランプ機能により本装置のランプを消灯しています。

【対処】 ランプを点灯させる場合は、lamp modeコマンドで運用中にランプを点灯する設定に変更後に本装置を再起動するか、または、ECOモードランプ機能でランプを点灯してください。
本装置が現在動作している設定は、show running-config lamp modeコマンド、ECOモードランプ機能による制御状態は、show system funcswitchコマンドで確認できます。

☛参照 コマンドリファレンス-運用管理編-「show running-config」、「show system funcswitch」
機能説明書「2.44 ECOモードランプ機能」（P.160）

● telnetで本装置のIPアドレスを指定したがうまくつながらない

【原因】 パソコンのIPアドレスやネットマスクが間違っています。

【対処】
- パソコンの設定でIPアドレスやネットマスクを設定している場合は、本装置と通信できるIPアドレスが設定されているかどうかを確認してください。
  本装置のIPアドレスやネットマスクを変更していない場合は、パソコンには以下の範囲で設定する必要があります。
  IPアドレス　：192.168.1.2～192.168.1.254
  ネットマスク　：255.255.255.0
- 本装置のDHCPサーバ機能を利用している場合は、パソコンを再起動してください。

補足 パソコン側のIP設定は、ipconfigコマンド（Windows 2000／Windows XP／Windows Vista／Windows 7／Windows NTの場合）で確認できます。

【原因】 パソコンとTAでインターネットに接続したときの設定が残っています。

【対処】 LANインタフェースのIPアドレスを再割り当てするため、パソコンを再起動してください。

【原因】 ETHERグループ2以外のポートに接続されています。

【対処】 本装置の設定を変更していない場合は、ETHERグループ2のポートで接続できる設定となっています。LANケーブルが本装置のETHERグループ2のポートに正しく差し込んであることを確認してください。

【原因】 パソコンのARPエントリの値がおかしくなっています。

【対処】 本装置と同じIPアドレスを持つ機器と通信した直後に、パソコンの電源を落とさないまま本装置へ接続を変更した場合は通信できません。しばらく待つか、パソコンを再起動してください。

【原因】 本装置と同じIPアドレスを持つ機器が接続されています。

【対処】 IPアドレスが重複している機器がLAN上に存在すると、正しく通信できません。
本装置から設定を行うパソコン以外を接続しているLANケーブルを外し、パソコンを再起動してください。

【原因】 本装置のIPアドレスが変更されています。

【対処】 変更後の本装置のIPアドレスを指定してください。

【原因】 パソコンのIPアドレスを変更していません。

【対処】 本装置のIPアドレスを変更した場合、必ずパソコン側のIPアドレスもそれに合わせて変更します。
パソコンのIPアドレスを本装置と直接通信可能なアドレスに変更してください。また、ネットマスクを本装置に設定した値と同じ値に設定してください。このとき、DNSサーバのIPアドレスも忘れずに入力してください。

● 変更した本装置のIPアドレスがわからなくなった

【対処】 コンソールでログインして、構成定義を確認してください。

● 本装置に設定したパスワードがわからなくなった

【対処】 本装置をご購入時の状態に戻してください。こうすることでパスワードを削除し、IPアドレスを「192.168.1.1」に戻すことができます。それまでに設定した内容はすべて消えてしまいますので、最初から設定し直してください。

参照 「5 ご購入時の状態に戻すには」（P.45）

- **他装置で使用している構成定義を設定しようとしても、暗号化パスワード文字列がエラーになって設定できない**

【原因】 他装置の構成定義にpassword format uniqueが設定されており、暗号化パスワード文字列が装置固有パスワード形式になっています。

【対処】 暗号化パスワード文字列を平文パスワード文字列に置き換え、続くencryptedの文字列を除いて設定してください。

- **装置を交換したあと、以前設定していた構成定義を再設定しようとしても、暗号化パスワード文字列がエラーになって設定できない**

【原因】 以前の構成定義にpassword format uniqueが設定されており、暗号化パスワード文字列が装置固有パスワード形式になっています。

【対処】 暗号化パスワード文字列を平文パスワード文字列に置き換え、続くencryptedの文字列を除いて設定してください。

2.3 回線への接続に関するトラブル

本装置で回線に接続する際のトラブルには、以下のようなものがあります。

- **Windows NT 4.0でネットワークにログインするたびに回線が勝手につながってしまう**

【原因】 Remote Access Service（RAS）機能の設定が原因です。

【対処】 以下の手順で設定を変更してください。

1）［スタート］－［コントロールパネル］をクリックします。
2）［サービス］アイコンをダブルクリックして開きます。
3）一覧から「Remote Access Autodial Manager」を選択し、［停止］ボタンをクリックします。
4）［スタートアップ］をクリックし、「手動」か「無効」を選択します。

- **Windowsのアクティブデスクトップを使用すると、ときどき回線が自動的につながってしまう**

【原因】 アクティブデスクトップのInternet Explorerチャンネルバーの中のサイトを「購読」する設定になっているなどの原因が考えられます。

【対処】 以下の手順で設定を変更してください。

1）Internet Explorerを起動します。
2）メニューバーの［お気に入り］をクリックします。
3）［購読の管理］をクリックします。
4）選択されているチャンネルを削除します。

● 回線への接続に失敗する
システムログ情報を見ると「autodial locked by redial」というシステムログが連続して表示される

【原因】 回線側への通信を契機とした自動発信処理が行われましたが、3分間に2回を超えて回線接続に失敗しているため、発信がロックされています。
回線接続に失敗している要因としては以下が考えられます。

- 相手先番号に誤りがあります。
- 送信認証情報に誤りがあります。

【対処】 以下の構成定義が正しい情報で定義されているか確認してください。

- 接続先の電話番号の設定

```
remote [<number>] ap [<ap_number>] dial <count> number <dial_number>
```

- 送信認証情報の設定

```
remote [<number>] ap [<ap_number>] ppp auth send <id> <password> [encrypted]
```

また、システムログ情報の重複メッセージ出力の設定を「yes」にすることで、連続しての表示を抑止できます。

```
syslog dupcut yes
```

2.4 データ通信に関するトラブル

本装置でデータ通信を行う際のトラブルには、以下のようなものがあります。

● 回線はつながるが、データ通信ができない

【原因】 IPフィルタリング、NATまたは経路情報（本装置／相手）の設定が間違っています。

【対処】 IPフィルタリングの設定やNATの設定を、ご利用のネットワーク環境や目的に合わせて正しく設定し直してください。

【原因】 ETHERNETの転送レートの自動認識に失敗しました。

【対処】 本装置のETHERポートのランプの状態と接続しているHUB装置のLINK状態を確認します。両者の表示が異なっている場合は自動認識に失敗しています。本装置の転送レートをHUB装置の仕様に合わせた転送レート（1000Mbps-全二重、100Mbps-全二重、10Mbps-全二重、100Mbps-半二重、10Mbps-半二重）に変更し、再接続してください。

● 回線は接続されてPingの応答は正常だが、WWWブラウザや電子メールは通信できない

【原因】 DNSの設定が間違っています。

【対処】 本装置のDHCPサーバおよびProxyDNSを使用するか、パソコン側でDNSサーバのアドレスを正しく設定し直してください。

● ブラウザを立ち上げると勝手に回線が接続されてしまう

【原因】 ブラウザ起動時にインターネット上のページを表示するよう指定しています。

【対処】 ブラウザ起動時に表示されるページに何も指定しないか、ローカルディスク上のファイルを指定してください。

● 回線は接続されるが「このサーバに対するDNS項目がありません」などメッセージが表示されてブラウザの表示が止まってしまう

【原因】 DHCPサーバ機能を利用している場合、本装置の設定終了直後はパソコン側にDNSアドレス情報が含まれていないため、WWWブラウザでURL「http://www.fujitsu.com」を入力したときに「www.fujitsu.com」のIPアドレスを取り出せず、このようなメッセージが表示されます。

【対処】 パソコンを再起動して、DHCP（DNSサーバのIPアドレス）の最新情報をパソコン側に確実に反映させてください。

【原因】 DHCPサーバ機能を利用していない場合、DNSサーバのIPアドレスを手入力する必要があります。

【対処】 マニュアルに記載されている情報（IPアドレス、ネットマスク、ゲートウェイ）に加え、DNSサーバのIPアドレスを設定してください。

● 本装置のIPアドレスを変更し、再起動したら、まったくつながらなくなった

【原因】 DHCPの設定が古いです。

【対処】 IPアドレスを変更すると、DHCPの割り当て先頭IPアドレスが書き換わらないため、個別に設定を変更する必要があります。

● ルータ設定でIPアドレスを変更し、再起動したら、まったくつながらなくなった

【原因】 DHCPの設定が古いです。

【対処】 かんたん設定の場合、IPアドレスを変更すると、連動してDHCPの割り当て先頭IPアドレスが書き換わりますが、ルータ設定の場合、連動しないため、個別に設定を変更する必要があります。以下に例を示します。

例）本装置のIPアドレスを「192.168.1.1」から「172.32.100.1」に変更した場合

	［変更前］		［変更後］	
	IPアドレス	DHCP先頭IPアドレス	IPアドレス	DHCP先頭IPアドレス
かんたん設定	192.168.1.1	192.168.1.2	172.32.100.1	172.32.100.2
ルータ設定	192.168.1.1	192.168.1.2	172.32.100.1	192.168.1.2

● PPPoEで接続できない

【原因】 前回の接続中にルータの電源を切断したり、ADSLモデムとつながっているケーブルを抜くなどして、正常な切断処理を行わずにPPPoEセッションが切断されました。

【対処】 通信事業者側のPPPoEサーバが、まだ前回の接続が切断したことを認識していない場合があります。しばらく待ってから、再度、接続してください。

【原因】 アクセスコンセントレータ名やサービス名を入力しています。

【対処】 通信事業者からの指示がない限り、アクセスコンセントレータ名やサービス名を入力しないでください。

【原因】 フレッツ・ADSLの場合、ユーザ認証IDに＠以下を入力し忘れています。

【対処】 フレッツ・ADSLのユーザ認証IDは「xxx@xxx.ne.jp」や「xxx@xxx.com」のような形式を使用しています。契約しているプロバイダの指示に合わせて＠以下も入力してください。

【原因】 ADSLモデムと本装置との接続のしかたがおかしいためリンクが確立していません。

【対処】 ADSLモデムと本装置との間でリンクが確立していることを確認してください。ADSLモデムにリバーススイッチがついている場合、スイッチの設定が間違っている可能性があります。ADSLモデムの説明書に従ってスイッチを設定してください。

2.5 導入に関するトラブル

ネットワークに本装置を導入する際のトラブルには、以下のようなものがあります。

● プライベートLANを構築できない

【原因】 プライベートLAN側に接続されたパソコンに固定IPアドレスが設定されています。

【対処】 本装置のDHCPサーバ機能を利用するLAN側のパソコンは、IPアドレスを自動的に取得する設定にしてください。固定のIPアドレスを設定していると、本装置が配布するIPアドレスと重なり、矛盾が生じる場合があります。
本装置のIPアドレスを変更した場合、以下の2つの操作を行ってください。

- 本装置に接続しているパソコンのIPアドレスも本装置のIPアドレスに合わせて変更する必要があります。DHCPサーバ機能を使用して、再度IPアドレスを割り当ててください。
- 再起動後に本装置にアクセスするために、telnetで指定するIPアドレスに変更後のIPアドレスを指定してください。

● インターネットへPPPoEで接続できない

【原因】 物理LANインタフェースの転送レートを含むLAN情報が保存されていません。

【対処】 PPPoEを利用する物理インタフェースのLAN情報設定で、転送レートを必ず設定してください。
転送レートが設定されずに、その他のLAN情報で設定する値もすべて初期値の場合、そのLAN情報は保存されないため、通信できません。

● IPv6の事業所LANをIPv6 over IPv4トンネルで接続できない

【原因】 相手情報のMTUが不適切でカプセル化されたIPv4パケットのフラグメントが発生しています。

【対処】 利用する相手情報のMTUを1280に設定してください。

● 複数の事業所LANをIP-VPN網を利用して接続できない

【原因】 BGP機能とNAT機能を併用する設定になっています。

【対処】 BGP機能とNAT機能は併用できません。NAT機能の設定を変更してください。
初期設定ではNAT機能を使用する設定になっています。

2.6 IPsec/IKEに関するトラブル

IPsec/IKE通信を行う際のトラブルには、以下のようなものがあります。

● IPsec/IKE定義を複数行うと接続できない拠点がある

【原因】 各拠点の装置または相手情報のネットワーク情報（接続先情報）が複数定義されている装置のIPsec情報の対象パケットが他拠点と重なっています。

【対処】 相手情報のネットワーク情報（接続先情報）で自側／相手側エンドポイントが各拠点で誤りがないか確認してください。また、相手情報のネットワーク情報（接続先情報）が複数定義されている装置のIPsec情報の対象パケットが重ならないようにしてください。

【原因】 可変IPアドレスのVPN接続で、Responder（相手装置が可変IPアドレス）の定義をしている装置の各拠点の相手情報のネットワーク情報（接続先情報）の相手装置識別情報が重複しています。

【対処】 相手情報のネットワーク情報（接続先情報）の相手装置識別情報が異なるように設定してください。

● IKEネゴシエーションのLifeTimeが互いに異なる

【原因】 相手情報のネットワーク情報（接続先情報）のIKE情報またはIPsec情報のSA有効時間が装置間で異なっています。

【対処】 互いの装置の定義を確認して相手情報のネットワーク情報（接続先情報）のIKE情報またはIPsec情報のSA有効時間を合わせてください。

● Aggressive Mode設定を行ってもIKEネゴシエーションが開始されない

【原因】 可変IPアドレスのVPN接続でResponder（相手装置が可変IPアドレス）の定義をしている装置からIKEネゴシエーションを開始しようとしています。

【対処】 Initiator（自装置が可変IPアドレス）の定義をしている装置からIPsec対象となる装置に対しpingなどの疎通確認により、IKEネゴシエーションを開始するようにしてください。

● IPsec SAが存在するのに接続先セッション監視がダウンした

【原因】 監視先装置がネットワークに接続されていません。

【対処】 監視先装置をネットワークに接続するか、すでに接続されている装置を指定してください。

【原因】 接続先セッション監視パケットの応答経路が監視先装置にありません。

【対処】 経路を設定してください。

【原因】 通信負荷が高い、または回線品質が悪いです。

【対処】 接続先セッション監視パケットが最優先されるように、相手情報のネットワーク情報（接続先情報）の帯域制御情報（IP関連）を設定してください。

● IPsec SAは存在するが、IKE SAが存在しない

【原因】 相手IKEセッションから削除ペイロードを受信しました。

【対処】 対処の必要はありません。次回のIPsec SAの更新（Rekey）時にIKE SAが作成されます。

【原因】 IPsec SAが存在するときにIKE SAがSA有効時間を満了して解放されました。

【対処】 対処の必要はありません。次回のIPsec SAの更新（Rekey）時にIKE SAが作成されます。

● IKEネゴシエーション後に同一相手にもかかわらず複数のIPsec SAおよびIKE SAが作成される

【原因】 相手IKEセッションとIPsec SAの更新（Rekey開始）時間が同じです。

【対処】 相手情報のネットワーク情報（接続先情報）のIPsec情報のSA更新（Initiator時／Responder時）を装置間で異なるように設定してください。

● 互いの装置から最初のIKEネゴシエーションを同時に行うとIKEネゴシエーションに失敗する

【原因】 互いの装置から送信したInitial-Contactメッセージにより互い違いのIKE SAが残っています。

【対処】 接続優先制御の設定を一方の装置で「Initiatorを優先」、一方の装置で「Responderを優先」のように互いの装置で異なる設定にしてください。

● IPsec化される前の帯域制御が行われない

【原因】 IPsec/IKE接続定義をしている相手情報のネットワーク情報（共通情報）でシェーピングが設定されていません。

【対処】 IPsec/IKE接続定義をしている相手情報のネットワーク情報（共通情報）でシェーピングを設定してください。
使用するインタフェースがlanインタフェースの場合は、シェーピングを使用することで帯域制御機能が有効に動作します。

【原因】 相手情報のネットワーク情報（接続先情報）の帯域制御情報（IP関連）の対象範囲が相手情報のネットワーク情報（接続先情報）のIPsec情報の対象パケットに含まれていません。

【対処】 相手情報のネットワーク情報（接続先情報）の帯域制御情報（IP関連）の対象範囲が相手情報のネットワーク情報（接続先情報）のIPsec情報の対象パケットに含まれるように設定してください。

● 手動鍵設定でIPsec通信ができない

【原因】 自装置の手動鍵送信用IPsec情報のセキュリティパラメタインデックスのSPIと相手装置の手動鍵受信用IPsec情報のSPI、または自装置の手動鍵受信用IPsec情報のSPIと相手装置の手動鍵送信用IPsec情報のSPIが一致していません。

【対処】 自装置の手動鍵送信用IPsec情報のSPIと相手装置の手動鍵受信用IPsec情報のSPI、または自装置の手動鍵受信用IPsec情報のSPIと相手装置の手動鍵送信用IPsec情報のSPIを合わせてください。

【原因】 自装置の手動鍵送信用IPsec情報のセキュリティプロトコルと相手装置の手動鍵受信用IPsec情報のセキュリティプロトコル、または自装置の手動鍵受信用IPsec情報のセキュリティプロトコルと相手装置の手動鍵送信用IPsec情報のセキュリティプロトコルが一致していません。

【対処】 自装置の手動鍵送信用IPsec情報のセキュリティプロトコルと相手装置の手動鍵受信用IPsec情報のセキュリティプロトコル、または自装置の手動鍵受信用IPsec情報のセキュリティプロトコルと相手装置の手動鍵送信用IPsec情報のセキュリティプロトコルを合わせてください。

【原因】 自装置の手動鍵送信用IPsec情報の対象範囲と相手装置の手動鍵受信用IPsec情報の対象範囲、または自装置の手動鍵受信用IPsec情報の対象範囲と相手装置の手動鍵送信用IPsec情報の対象範囲が一致していません。

【対処】 自装置の手動鍵送信用IPsec情報の対象範囲と相手装置の手動鍵受信用IPsec情報の対象範囲、または自装置の手動鍵受信用IPsec情報の対象範囲と相手装置の手動鍵送信用IPsec情報の対象範囲を合わせてください。

【原因】 自装置の手動鍵送信用IPsec情報の暗号情報／認証情報と相手装置の手動鍵受信用IPsec情報の暗号情報／認証情報、または自装置の手動鍵受信用IPsec情報の暗号情報／認証情報と相手装置の手動鍵送信用IPsec情報の暗号情報／認証情報が一致していません。

【対処】 自装置の手動鍵送信用IPsec情報の暗号情報／認証情報と相手装置の手動鍵受信用IPsec情報の暗号情報／認証情報、または自装置の手動鍵受信用IPsec情報の暗号情報／認証情報と相手装置の手動鍵送信用IPsec情報の暗号情報／認証情報を合わせてください。鍵には、文字列鍵と16進数鍵があるので注意してください。

【原因】 トンネル利用時の自側／相手側のトンネルエンドポイントアドレス（IPsecトンネル）パケットが手動鍵送受信用IPsec情報の対象範囲パケットと同じインタフェースから送受信するようになっています。

【対処】 IPsecトンネルパケットと手動鍵送受信用IPsec情報の対象範囲パケットが別のインタフェースから送受信するように設定してください。

● IKE ネゴシエーション後に同一相手にかかわらず複数の IPsec SA および IKE SA が作成される

【原因】 互いの装置から同時に IKE ネゴシエーションが行われました。

【対処】 対処の必要はありません。次回の IPsec SA の更新（Rekey）および IPsec 通信に影響はありません。

● 手動鍵設定の暗号アルゴリズムが互いの装置で des-cbc と 3des-cbc の場合にもかかわらず IPsec 通信できた

【原因】 3des-cbc の暗号鍵を 16 桁ごとに 3 つに分割した鍵が、des-cbc の暗号鍵と同じ鍵になっています。

【対処】 アルゴリズムは、トンネルの往路または復路で同じものを設定してください。また、暗号アルゴリズムに 3des を選択する場合は、以下のように鍵を 16 桁ごとに 3 つに分割し、鍵 1 ≠鍵 2 ≠鍵 3 となるように鍵を設定してください。

鍵 :1122334455667788　9900aabbccddeeff　1122334455667788

鍵 1（16 桁）　鍵 2（16 桁）　鍵 3（16 桁）

鍵 1 ＝鍵 3 のように鍵を設定すると、16 バイトの鍵で暗号化するのと同じ結果になります。また、鍵 1 ＝鍵 2、鍵 2 ＝鍵 3 のように鍵を設定すると、それぞれ鍵 3、鍵 1 の des-cbc 暗号と同じ結果になります（鍵 1 ＝鍵 2 ＝鍵 3 の場合も同様です）。

● テンプレート着信機能（AAA 認証または RADIUS 認証）を使用した IPsec/IKE 定義を行うと IKE ネゴシエーションが開始されない

【原因】 テンプレート着信機能（AAA 認証または RADIUS 認証）を使用した IPsec/IKE 定義を行っている装置から IKE ネゴシエーションを開始しようとしています。

【対処】 テンプレート着信機能（AAA 認証または RADIUS 認証）を使用して VPN 接続を行う相手装置から ping などの疎通確認により、IKE ネゴシエーションを開始するようにしてください。

● テンプレート着信機能（AAA 認証または RADIUS 認証）を使用した IPsec/IKE 定義を行うと接続できない

【原因】 AAA 認証または RADIUS 認証で失敗しています。

【対処】 以下のどれかに該当していないか確認してください。

- AAA の設定または RADIUS 認証サーバへ認証 ID および認証パスワードを設定していない場合は、認証 ID および認証パスワードを設定してください。
- AAA の設定または RADIUS 認証サーバへ登録している認証 ID と認証パスワードが異なっている可能性があります。認証 ID と認証パスワードは同じものを設定してください。
- 相手装置の認証 ID（Aggressive Mode の場合は装置識別情報、Main Mode の場合は IPsec トンネルアドレスを示す）と AAA または RADIUS 認証サーバの設定が異なっている場合、どちらも同じ認証 ID を設定してください。
- IPv6 トンネルの構成で IPv6 トンネルアドレスを認証 ID および認証パスワードとした場合、IPv6 アドレスを省略して記述しないでください。省略なしの IPv6 アドレスを認証 ID および認証パスワードとして設定してください。
- RADIUS 認証を設定している場合、RADIUS 認証サーバへ通信が行えていることを確認してください。

【原因】 AAA 設定または RADIUS 認証サーバへ登録している IKE 情報の共有鍵と接続相手の IKE 情報の共有鍵が一致していません。

【対処】 AAA 設定または RADIUS 認証サーバへ接続相手と同じ共有鍵を設定してください。

【原因】 AAA 設定または RADIUS 認証サーバへ登録している情報が不足しています。

【対処】 AAA 設定または RADIUS 認証サーバへ必要な以下の情報を設定してください。

- 認証 ID
- 認証パスワード
- 共有鍵
- IPsec 対象範囲
  ただし AAA の設定に限り、送信元 IP アドレスおよびあて先 IP アドレスは、すべての IPv4 アドレスを IPsec 対象に含める場合、初期設定のため設定する必要はありません。
- スタティック経路情報

● テンプレート着信機能（AAA 認証または RADIUS 認証）を使用した IPsec/IKE 定義を行うと IPsec SA が存在するのに暗号化されない

【原因】 AAA 設定または RADIUS 認証サーバへ登録しているスタティック経路情報に誤りがあります。または、スタティック経路情報がありません。

【対処】 AAA 設定または RADIUS 認証サーバへ登録しているスタティック経路情報に誤りがないことを確認して設定してください。

【原因】 IPsec 対象パケットが IPv6 アドレスでテンプレート情報の IPv6 機能の設定が off になっています。

【対処】 テンプレート情報の IPv6 機能を on に設定してください。

【原因】 AAA 設定のスタティック経路情報がアクセスインタフェースに存在しません。

【対処】 AAA 設定のスタティック経路情報をほかのインタフェースと重複しないように設定してください。

● テンプレート着信機能（AAA 認証または RADIUS 認証）を使用した IPsec/IKE 定義を行うと IPsec SA が存在するのに通信できない

【原因】 AAA 設定または RADIUS 認証サーバへ登録している IPsec 対象範囲に誤りがあります。

【対処】 AAA 設定または RADIUS 認証サーバへ登録している IPsec 対象範囲に誤りがないことを確認して設定してください。

● テンプレート着信機能（AAA 認証または RADIUS 認証）を使用した IPsec/IKE 定義を行うとテンプレートの接続先監視機能が動作しない

【原因】 AAA 設定または RADIUS 認証サーバへ登録している接続先監視アドレス、および、テンプレートに設定している接続先監視アドレスのどちらか一方しか設定していません。

【対処】 AAA 設定または RADIUS 認証サーバへ登録している接続先監視アドレス、および、テンプレート定義に設定している接続先監視アドレスの両方を設定してください。

● テンプレート着信機能（動的 VPN）を使用した IPsec/IKE 定義を行うと接続できない

【原因】 テンプレート着信機能（動的 VPN）を使用した IPsec/IKE 定義を行うための情報に誤りがあります。または、不足しています。

【対処】 テンプレート着信機能（動的 VPN）を使用した IPsec/IKE 定義情報を確認して正しく設定してください。

【原因】 自側ユーザ ID が動的 VPN サーバに登録されていません。

【対処】 動的 VPN サーバへの通信が行えることを確認してください。

【原因】 接続相手のユーザ ID が動的 VPN サーバに登録されていません。

【対処】 接続相手のユーザ ID が動的 VPN サーバに登録してください。登録されるまで動的 VPN で接続することができません。

【原因】 動的 VPN 接続契機パケットの検出条件が設定されていない、または設定に誤りがあります。

【対処】 動的 VPN 接続契機パケットの検出条件を確認し、正しく設定してください。

【原因】 IPsecまたはIKE情報のどちらかが接続相手と一致していません。

【対処】 以下の設定が接続相手と同じになるように設定してください。

- 自動鍵交換用IPsec情報のセキュリティプロトコルの設定
- 自動鍵交換用IPsec情報の暗号情報の設定
- 自動鍵交換用IPsec情報の認証情報の設定
- 自動鍵交換用IPsec情報のPFS使用時のDH（Diffie-Hellman）グループの設定
- IKEセッション確立時の共有鍵（Pre-shared key）の設定
- IKEセッション用暗号情報の設定

【原因】 動的VPN情報交換で取得した相手IPsecトンネルアドレスに対し、優先度の高い経路がすでに存在します。

【対処】 対象となる既存経路の優先度を下げてください。

【原因】 静的経路数が最大数を超えたため、動的VPN情報交換で取得した相手IPsecトンネルアドレスに対する経路が追加できませんでした。

【対処】 静的経路を確認してください。

● テンプレート着信機能（動的VPN）を使用したIPsec/IKE定義を行うとIPsec SAが存在していても拠点間通信ができない

【原因】 IPsec対象パケットがIPv6アドレスでテンプレート情報のIPv6機能の設定がoffになっています。

【対処】 テンプレート情報のIPv6機能をonに設定してください。

● テンプレート着信機能（動的VPN）を使用して接続先監視ができない

【原因】 本装置または相手装置のどちらかに接続先監視の定義がされていません。

【対処】 接続先監視を行う場合は、両方の装置で設定してください。

● NATトラバーサルを使用したIPsec/IKE機能が動作しない

【原因】 IKE区間にNAT装置が存在しません。

【対処】 NATトラバーサルは、IKE区間にNAT装置を検出したときだけ動作します。

【原因】 セキュリティプロトコルに認証（AH）を指定しています。

【対処】 NATトラバーサルでは、セキュリティプロトコルは暗号（ESP）しかサポートしていません。セキュリティプロトコルを暗号（ESP）で指定するように定義を変更してください。

● NATトラバーサルを使用したIKEネゴシエーションに失敗する

【原因】 動的VPN機能を使用したIPsec/IKE定義を設定しています。

【対処】 動的VPNは未サポートのため使用できません。

【原因】 両装置でサポートするベンダIDが一致していません。

【対処】 以下のベンダIDだけをサポートしています。対抗装置が以下をサポートしていない場合は、NATトラバーサルは使用できません。

- RFC 3947
- draft-ietf-ipsec-nat-t-ike-03
- draft-ietf-ipsec-nat-t-ike-02\n
- draft-ietf-ipsec-nat-t-ike-02

IPsec設定ミス　トラブルシュート方法

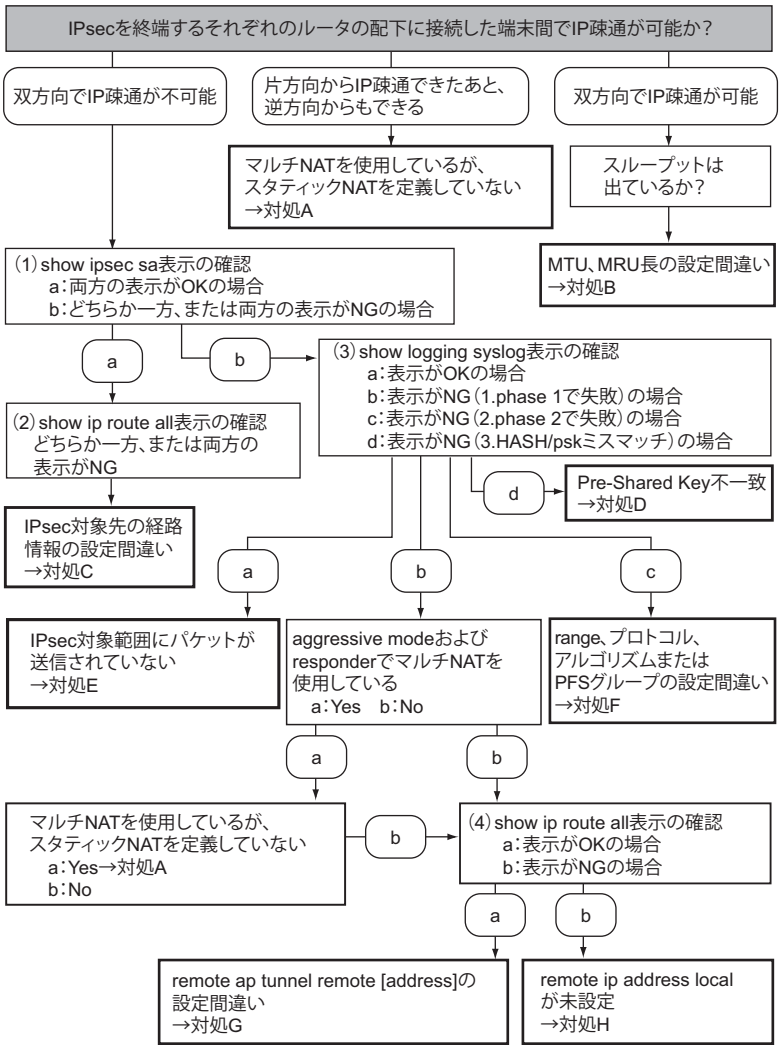
IPsecの設定ミスの原因と対処を、以下のフローチャートで特定してください。

フローチャート内の（1）～（4）は「 ログ表示の確認」（P.24）の（1）～（4）に対応しています。各項目のOK表示例およびNG表示例を確認し、a～dのあてはまる項目へ進みます。

また、対処A～Hは「 対処方法」（P.29）の対処A～Hに対応しています。

こんな事に気をつけて

ここで解説しているトラブルシュート方法は、IPsec接続に限定した記述であり、PPPoE接続などの下位レイヤ接続はすでに確立していることを前提としています。また、接続形態や構成により接続できない原因は多様であるため、設定ミスの特定もあくまでミスの可能性を示すものであり、必ずしも断定的なものではありません。



ログ表示の確認

ログのOK表示例とNG表示例を、フローチャート内の（1）～（4）の順に説明します。

IPsecを終端しているそれぞれのルータで確認してください。

（1）show ipsec sa表示を確認

OKの場合の表示例

IPsec SAがIN、OUTそれぞれ1つ以上、IKE SAが1つ以上表示される。

```
# show ipsec sa
[IPsec SA Information]
[1]             Remote Name(IPsec), rmt0, ap0
                Side(Initiator), Gateway(10.1.1.2, 10.1.1.1), OUT
                Protocol(ESP), Enctype(3des-cbc), Authtype(hmac-sha1), PFS(modp768)
                Status(mature), Spi=88893807(0x054c696f)
                Created(Jan 25 17:56:47 2011), NewSA(28710secs, 0Kbyte)
                Lifetime(28800secs), Current(2secs), Remain(28798secs)
                Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[2]             Remote Name(IPsec), rmt0, ap0
                Side(Initiator), Gateway(10.1.1.1, 10.1.1.2), IN
                Protocol(ESP), Enctype(3des-cbc), Authtype(hmac-sha1), PFS(modp768)
                Status(mature), Spi=267160340(0x0fec8b14)
                Created(Jan 25 17:56:47 2011), NewSA(28710secs, 0Kbyte)
                Lifetime(28800secs), Current(2secs), Remain(28798secs)
                Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[IKE SA Information]
[1]             Destination(10.1.1.2.500), Source(10.1.1.1.500), rmt0
                Cookies(5b2023b77ea4c7de:68dd6596e28e7aa3)
                Side(Initiator), Status(ESTABLISHED), Exchangetype(MAIN)
                IKE Version(1), Authmethod(shared-key), DPD(disable)
                 Enctype(3des-cbc), Hashtype(hmac-sha1), PFS(modp768)
                Created(Jan 25 17:56:46 2011)
                Lifetime(86400secs), Current(3secs), Remain(86397secs)

#
```

NGの場合の表示例

IPsec SAが表示されない、およびIKE SAが1つだけ表示され、Cookiesの後半がすべて0となっている。

```
# show ipsec sa
[IKE SA Information]
[1]             Destination(10.1.1.2.500), Source(10.1.1.1.500), rmt0
                Cookies(0727e870341cd187:0000000000000000)
                Side(Initiator), Status(MSG1SENT), Exchangetype(MAIN)
                IKE Version(1), Authmethod( ), DPD(disable)
                Enctype( ), Hashtype( ), PFS( )
                Created( )
                Lifetime(0secs), Current(0secs), Remain(0secs)

#
#show ipsec sa
#
```

(2)show ip route all表示の確認

OKの場合の表示例

IPsec通信対象のあて先ネットワークアドレスが、IPsecインタフェースに向いている。

以下の例では、IPsecインタフェースはremote 1であり、IPsec対象である対向ルータLAN側ネットワークアドレス192.168.2.0/24がスタティックで有効になっている。

```
# show ip route all
FP    Destination/Mask    Gateway        Distance      UpTime      Interface
*S    0.0.0.0/0           rmt0                  0     00:01:03    rmt0
*L    10.1.1.1/32         10.1.1.1              0     00:03:49    rmt0
*C    192.168.1.0/24      192.168.1.1           0     00:03:49    lan1
*S    192.168.2.0/24      rmt1                  0     00:01:03    rmt1
#
```

NGの場合の表示例

IPsec通信対象のあて先ネットワークアドレスが、IPsecインタフェースに向いていない。

以下の例では、IPsecインタフェースはremote 1であり、IPsec対象のあて先は対向ルータLAN側ネットワークアドレス192.168.2.0/24であるが、デフォルトルートに一致するためremote 0のPPPoEインタフェースにルーティングされる（IPsec暗号化されない）。

```
# show ip route all
FP    Destination/Mask    Gateway        Distance      UpTime      Interface
*S    0.0.0.0/0           rmt0                  0     00:01:03    rmt0
*L    10.1.1.1/32         10.1.1.1              0     00:03:49    rmt0
*C    192.168.1.0/24      192.168.1.1           0     00:03:49    lan1
#
```

(3)show logging syslog表示の確認

OKの場合の表示例

以下のようにIPsec/IKE関連のメッセージが表示されない。

```
# show logging syslog
Mar 08 06:59:52 192.168.1.1 Si-R G200: init: system startup now.
Mar 08 06:59:52 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Mar 08 06:59:52 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Mar 08 06:59:52 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Mar 08 06:59:52 192.168.1.1 Si-R G200: protocol: lan 1 link up
Mar 08 06:59:52 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Mar 08 06:59:52 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
#
```

NGの場合の表示例

1.phase 1で失敗

表示内に"**isakmp:give up phase1 negotiation.**"が表示されている。

ただし、"isakmp:HASH mismatched"または"isakmp:psk mismatched"が表示されている場合は「3.HASH/psk/certificateミスマッチ」（P.27）を参照してください。

```
# show logging syslog
Jan 01 09:23:53 192.168.1.1 Si-R G200: init: system startup now.
Jan 01 09:23:53 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Jan 01 09:23:53 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Jan 01 09:23:53 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Jan 01 09:23:53 192.168.1.1 Si-R G200: protocol: lan 1 link up
Jan 01 09:23:53 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Jan 01 09:23:53 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
Jan 01 09:25:04 192.168.1.1 Si-R G200: isakmp: give up phase1 negotiation. 10.1.2.1[500] -> 10.1.1.1[500]
#
```

2.phase 2で失敗

表示内に"**isakmp: give up phase2 negotiation.**"が表示されている。

Initiator

```
# show logging syslog
Apr 28 14:31:29 192.168.1.1 Si-R G200: init: system startup now.
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: lan 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
Apr 28 14:32:24 192.168.1.1 Si-R G200: isakmp: give up phase2 negotiation. 10.1.2.1[500] -> 10.1.1.1[500]
#
```

Responder

- range間違いは、syslogの出力はない

```
# show logging syslog
Apr 28 14:31:29 192.168.1.1 Si-R G200: init: system startup now.
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: lan 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
#
```

- プロトコル間違いは、syslogの出力はない

```
# show logging syslog
Apr 28 14:31:29 192.168.1.1 Si-R G200: init: system startup now.
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: lan 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
#
```

- 暗号アルゴリズム間違い

```
# show logging syslog
Apr 28 14:31:29 192.168.1.1 Si-R G200: init: system startup now.
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: lan 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
Apr 28 14:34:04 192.168.1.1 Si-R G200: isakmp: IPsec SA encryption algorithm mismatched.
Apr 28 14:34:14 192.168.1.1 Si-R G200: isakmp: IPsec SA encryption algorithm mismatched.
#
```

- 認証アルゴリズム間違い

```
# show logging syslog
Apr 28 14:31:29 192.168.1.1 Si-R G200: init: system startup now.
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: lan 1 link up
Apr 28 14:31:29 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Apr 28 14:31:29 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
Apr 28 14:35:32 192.168.1.1 Si-R G200: isakmp: IPsec SA authentication algorithm mismatched.
Apr 28 14:35:42 192.168.1.1 Si-R G200: isakmp: IPsec SA authentication algorithm mismatched.
#
```

3.HASH/psk/certificate ミスマッチ

HASH mismatched、psk mismatched、certificate mismatched、signature mismatched は、Aggressive Mode の場合 Initiator で、Main Mode の場合 Responder で確認する。

- Aggressive Mode Initiator の場合、以下の太字行に、受信した HASH 値と受信パケットから生成した HASH 値が一致しないことを示すメッセージが表示されている。

```
# show logging syslog
Jan 01 04:35:36 192.168.1.1 Si-R G200: init: system startup now.
Jan 01 04:35:36 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Jan 01 04:35:36 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Jan 01 04:35:36 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Jan 01 04:35:36 192.168.1.1 Si-R G200: protocol: lan 1 link up
Jan 01 04:35:36 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Jan 01 04:35:36 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
Jan 01 04:35:37 192.168.1.1 Si-R G200: isakmp: HASH mismatched side=0 exchange type=4 status=3.
Jan 01 04:35:46 192.168.1.1 Si-R G200: isakmp: HASH mismatched side=0 exchange type=4 status=3.
Jan 01 04:36:01 192.168.1.1 Si-R G200: isakmp: HASH mismatched side=0 exchange type=4 status=3.
Jan 01 04:36:21 192.168.1.1 Si-R G200: isakmp: HASH mismatched side=0 exchange type=4 status=3.
Jan 01 04:36:30 192.168.1.1 Si-R G200: isakmp: give up phase1 negotiation. sir -> 10.1.1.2[500]
#
```

- Main Mode Responderの場合、以下の太字行に共有鍵が一致していない可能性があることを示すメッセージが表示されている。

```
# show logging syslog
Apr 20 17:29:59 192.168.1.1 Si-R G200: init: system startup now.
Apr 20 17:29:59 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Apr 20 17:29:59 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Apr 20 17:29:59 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Apr 20 17:29:59 192.168.1.1 Si-R G200: protocol: lan 1 link up
Apr 20 17:29:59 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Apr 20 17:29:59 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
Apr 20 17:50:14 192.168.1.1 Si-R G200: isakmp: psk mismatched.
Apr 20 17:50:24 192.168.1.1 Si-R G200: isakmp: psk mismatched.
Apr 20 17:50:42 192.168.1.1 Si-R G200: isakmp: psk mismatched.
Apr 20 17:51:03 192.168.1.1 Si-R G200: isakmp: psk mismatched.
Apr 20 17:51:09 192.168.1.1 Si-R G200: isakmp: give up phase1 negotiation. 10.1.2.1[500] -> 10.1.1.1[500]
#
```

- Main Mode Responderの場合、以下の太字行に相手装置証明書が一致していない可能性があることを示すメッセージが表示されている。

```
# show logging syslog
Jun 16 15:09:55 192.168.1.1 Si-R G200: init: system startup now.
Jun 16 15:09:55 192.168.1.1 Si-R G200: sshd: generating public/private host key pair.
Jun 16 15:09:55 192.168.1.1 Si-R G200: protocol: ether 1 1 link up
Jun 16 15:09:55 192.168.1.1 Si-R G200: protocol: ether 1 2 link up
Jun 16 15:09:55 192.168.1.1 Si-R G200: protocol: lan 1 link up
Jun 16 15:09:55 192.168.1.1 Si-R G200: sshd: generated public/private host key pair.
Jun 16 15:09:55 192.168.1.1 Si-R G200: protocol: [vlan2] connected to PPPoE.pppoe() by keep connection
Jun 16 15:10:03 192.168.1.1 Si-R G200: isakmp: certificate mismatched. SIR.SIR
Jun 16 15:10:03 192.168.1.1 Si-R G200: isakmp: signature mismatched. SIR.SIR
Jun 16 15:10:13 192.168.1.1 Si-R G200: isakmp: certificate mismatched. SIR.SIR
Jun 16 15:10:13 192.168.1.1 Si-R G200: isakmp: signature mismatched. SIR.SIR
Jun 16 15:10:30 192.168.1.1 Si-R G200: isakmp: certificate mismatched. SIR.SIR
Jun 16 15:10:30 192.168.1.1 Si-R G200: isakmp: signature mismatched. SIR.SIR
Jun 16 15:11:23 192.168.1.1 Si-R G200: isakmp: give up phase1 negotiation. 10.1.2.1[500] -> 10.1.1.1[500]
#
```

(4)show ip route all表示の確認

OKの場合の表示例

自側IPsecトンネルエンドポイントのアドレス（ホストアドレス）が該当インタフェースに向いている。

以下の例では、10.1.1.1/32がPPPoEインタフェースremote 0で有効になっている。

```
# show ip route all
FP    Destination/Mask    Gateway        Distance      UpTime      Interface
*S    0.0.0.0/0           rmt0                  0     00:01:03    rmt0
*L    10.1.1.1/32         10.1.1.1              0     00:03:49    rmt0
*C    192.168.1.0/24      192.168.1.1           0     00:03:49    lan1
*S    192.168.2.0/24      rmt1                  0     00:01:03    rmt1
#
```

NGの場合の表示例

自側IPsecトンネルエンドポイントのアドレス（ホストアドレス）が該当インタフェースに向いていない。

以下の例では、自側エンドポイントアドレスは10.1.1.1であるが、表示されていない。

ただし、可変IPアドレスでのAggressive Modeの Initiatiorの場合は、以下の表示でも問題ない。

```
# show ip route all
FP    Destination/Mask    Gateway        Distance    UpTime      Interface
*S    0.0.0.0/0           rmt0                  0    00:01:03    rmt0
*C    192.168.1.0/24      192.168.1.1           0    00:03:49    lan1
*S    192.168.2.0/24      rmt1                  0    00:01:03    rmt1
#
```

対処方法

フローチャート内の対処A～Hについて、以下に説明します。

対処に合わせて設定を変更してください。なお、コマンド内の（本文）は表示されません。

- マルチNATを使用しているが、スタティックNATを定義していない→【対処A】（P.29）
- MTU、MRU長の設定間違い→【対処B】（P.30）
- IPsec対象先の経路情報の設定間違い→【対処C】（P.31）
- Pre-Shared Key不一致→【対処D】（P.31）
- IPsec対象範囲にパケットが送信されていない→【対処E】（P.32）
- range、プロトコル、アルゴリズムまたはPFSグループの設定間違い→【対処F】（P.32）
- remote ap tunnel remote [address]の設定間違い→【対処G】（P.33）
- remote ip address local が未設定→【対処H】（P.33）

【対処A】

インターネットVPNなどで、IPsec通信のほかにインターネット上のサーバなどと通信する場合、マルチNAT機能を使用する必要があります。マルチNAT機能を使用して、VPNで使用するアドレスがNATのアドレスプールに含まれる場合は、スタティックNATを指定してください。これはIPsec通信に用いられるアドレスが変換されてしまうのを防ぐためです。

設定例

Aggressive Mode Initiator PPPoEで割り当てられる可変アドレスでのVPNの場合

Aggressive Modeでは Initiatorだけがマルチ NAT機能だけを使用しているのであれば、IPsec SA自体は確立できますが、その後Responderから IPsecパケットを送信しなければNATテーブルが作成されず、通信できません。Responderでマルチ NAT機能だけを使用していると IPsec SAも確立されません。

Main Modeでは IKEのネゴシエーションを双方から開始するので、マルチ NAT機能だけを使用していても IPsec SAは確立されます。ただし、IPsec通信はNATテーブルが双方に作成されるまで不可能となります。

```
# ether 1 1 vlan untag 2
# ether 1 2 vlan untag 3
# lan 0 vlan 2
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 3
# remote 0 name ISP
# remote 0 mtu 1454
# remote 0 ap 0 name isp
# remote 0 ap 0 datalink bind vlan 2
# remote 0 ap 0 ppp auth send sir2 sir2
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
（NATを使用する場合は以下のスタティックNATが設定されているか確認する）
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17 IKE(UDP:500)
# remote 0 ip nat static 1 192.168.2.1 any any any 50 ESP(IP:50)
```

```
# remote 0 ip msschange 1414
# remote 1 name SIR
# remote 1 ap 0 name SIR
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike name local sir
# remote 1 ap 0 ike shared key text sir
# remote 1 ap 0 ike proposal 0 encrypt 3des-cbc
# remote 1 ap 0 tunnel remote 10.1.1.1
# remote 1 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
# remote 1 ip route 0 192.168.1.0/24 1 1
```

【対処 B】

フレッツ ADSL をアクセス回線としてインターネットに接続する場合、PPPoE ヘッダと PPP ヘッダが付加されるため、それを見積もった MTU/MSS を設定してください。PPPoE を設定しているインタフェースで、MTU=1454、MSS=1414 に設定していないと、通信がうまくいかなかったり、パケット分割して送信するため通常よりスループットが出ない場合があります。

設定例

```
# ether 1 1 vlan untag 2
# ether 1 2 vlan untag 3
# lan 0 vlan 2
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 3
# remote 0 name ISP
（以下の設定がされているか確認する）
# remote 0 mtu 1454
# remote 0 ap 0 name ISP
# remote 0 ap 0 datalink bind vlan 2
# remote 0 ap 0 ppp auth send sir2 sir2
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
（以下の設定がされているか確認する）
# remote 0 ip msschange 1414
# remote 1 name SIR
# remote 1 ap 0 name SIR
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike name local sir
# remote 1 ap 0 ike shared key text sir
# remote 1 ap 0 ike proposal 0 encrypt 3des-cbc
# remote 1 ap 0 tunnel remote 10.1.1.1
# remote 1 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
# remote 1 ip route 0 192.168.1.0/24 1 1
```

【対処 C】

IPsec 対象先のネットワークアドレスが、IPsec インタフェースに向いていないため、IPsec 対象先の経路情報を設定してください。

設定例

```
# show ip route all
FP    Destination/Mask    Gateway     Distance    UpTime     Interface
*S    0.0.0.0/0           rmt0               0    00:01:03   rmt0
*L    10.1.1.1/32         10.1.1.1           0    00:03:49   rmt0
*C    192.168.1.0/24      192.168.1.1        0    00:03:49   lan1
*S    192.168.2.0/24      rmt1               0    00:01:03   rmt1
#
```

【対処 D】

Pre-Shared Key 認証は IKE の認証方式で、IKE の相手と同じ秘密鍵を生成し、それを元に HASH 計算した値を交換することにより、認証を行います。これは Phase 1 で行われるので、本装置に設定した Pre-Shared Key が異なれば Phase 1 の IKE ネゴシエーションで失敗します。必ずそれぞれの IPsec 終端ルータで同じ鍵を設定してください。

設定例

```
# ether 1 1 vlan untag 2
# ether 1 2 vlan untag 3
# lan 0 vlan 2
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 3
# remote 0 name ISP
# remote 0 mtu 1454
# remote 0 ap 0 name ISP
# remote 0 ap 0 datalink bind vlan 2
# remote 0 ap 0 ppp auth send sir2 sir2
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip msschange 1414
# remote 1 name SIR
# remote 1 ap 0 name SIR
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike name local sir
（以下の設定が対向ルータと合っているか確認する）
# remote 1 ap 0 ike shared key text sir
# remote 1 ap 0 ike proposal 0 encrypt 3des-cbc
# remote 1 ap 0 tunnel remote 10.1.1.1
# remote 1 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
# remote 1 ip route 0 192.168.1.0/24 1 1
```

【対処 E】

IPsec/IKE 関連のメッセージが表示されない場合、IKE ネゴシエーションの送受信が行われていません。IPsec 対象範囲にパケットが送信されているか確認してください。

設定例

送信元アドレスが 192.168.1.0/24 のネットワーク内である場合

```
# remote 0 ap 0 ipsec ike range 192.168.1.0/24 any4
```

【対処 F】

IKE ネゴシエーションでは phase 2 で互いの IPsec 暗号化対象ネットワークアドレス（range）の交換を行います。それぞれの IPsec 終端ルータで送信元、あて先を逆に設定してください。

以下の設定では IPsec SA が確立できません。

```
ルータ A
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
ルータ B
# remote 1 ap 0 ipsec ike range 192.168.2.0/24 any4
```

以下の設定のように変更してください。

```
ルータ A
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 192.168.2.0/24
ルータ B
# remote 1 ap 0 ipsec ike range 192.168.2.0/24 192.168.1.0/24
```

```
ルータ A
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
ルータ B
# remote 1 ap 0 ipsec ike range any4 192.168.1.0/24
```

```
ルータ A
# remote 1 ap 0 ipsec ike range any4 any4
ルータ B
# remote 1 ap 0 ipsec ike range any4 any4
```

設定例

```
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec ike protocol esp
（以下の部分の設定が IPsec 対象先と矛盾していないか確認する）
# remote 1 ap 0 ipsec ike range 192.168.2.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ipsec type ike
```

【対処 G】

IPsec を終端する対向ルータの IP アドレス（トンネルエンドポイント）を設定してください。以下のように、モードによって必要な設定が異なる場合があります。

- Aggressive Mode の場合

  Initiator remote ap tunnel remote の設定

  Responder remote ap tunnel local の設定

- Main Mode の場合

  両方に remote ap tunnel local、remote ap tunnel remote の設定

設定例

```
# remote 1 name SIR
# remote 1 ap 0 name SIR
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike name local sir
# remote 1 ap 0 ike shared key text sir
# remote 1 ap 0 ike proposal 0 encrypt 3des-cbc
（以下の設定がきちんとされているか確認する）
# remote 1 ap 0 tunnel remote 10.1.1.1
# remote 1 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
# remote 1 ip route 0 192.168.1.0/24 1 1
```

【対処 H】

Main Mode の双方と Aggressive Mode の Responder で、必ず PPPoE インタフェースなどの、IPsec で暗号化されたパケットが送出されるように、インタフェースを設定してください。これはほとんどの場合（IPsec トンネルの途中に NAT 変換機器などが存在する場合を除く）、自側トンネルエンドポイントと同じアドレスが設定されます。

設定例

```
# ether 1 1 vlan untag 2
# ether 1 2 vlan untag 3
# lan 0 vlan 2
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 3
# remote 0 name ISP
# remote 0 mtu 1454
# remote 0 ap 0 name ISP
# remote 0 ap 0 datalink bind vlan 2
# remote 0 ap 0 ppp auth send sir sir
# remote 0 ap 0 keep connect
（Main Mode の場合、remote 1 ap 0 tunnel local で設定するアドレスが自インタフェースに設定されているか確認する）
# remote 0 ip address local 10.1.1.1
# remote 0 ip route 0 192.168.2.1/32 1 0
# remote 0 ip msschange 1414
# remote 1 name SIR
# remote 1 ap 0 name SIR
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
```

```
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text sir
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 tunnel local 10.1.1.1
# remote 1 ap 0 tunnel remote 10.1.1.2
# remote 1 ap 0 sessionwatch address 192.168.1.1 192.168.2.1
# remote 1 ap 0 sessionwatch interval 10s 3m 5s
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ip msschange 1414
```

2.7 認証機能に関するトラブル

IEEE802.1X 認証、MAC アドレス認証機能を利用する際のトラブルには、以下のようなものがあります。

● 認証ポートのリンクがアップしない（共通）

【原因】 認証で使用する AAA グループ定義が定義されていません。

【対処】 AAA グループの定義を追加してください。

【原因】 認証ポートに VLAN が定義されています。

【対処】 VLAN の定義を削除してください。

● 認証機能を併用したポートのリンクがアップしない

【原因】 併用する認証機能の認証方式が同一の定義でありません。

【対処】 認証方式の定義を同一の定義にしてください。

● 認証が成功しない（共通）

【原因】 RADIUS サーバの設定が誤っています。

【対処】 システムログで RADIUS サーバとの通信が失敗していることを示すログが採取されていないかを確認し、該当するログが採取されている場合は、以下の点に注意して RADIUS サーバの設定を見直してください。

- RADIUS サーバの IP アドレスと RADIUS サーバまでの経路情報
- RADIUS サーバのシークレット情報
- RADIUS サーバ側で許容する RADIUS クライアントアドレス

【原因】 RADIUS サーバで Supplicant が登録されていません。

【対処】 RADIUS サーバ側で登録されたユーザ情報を確認してください。

【原因】 本装置の Supplicant に割り当てる VLAN ID と同一の VLAN ID が設定されていません。

【対処】 以下のどちらかを設定してください。

- 割り当てる VLAN ID と同一の VLAN ID を持つポートを ether グループ 2 に設定してください。
- 認証割り当て用 VLAN として resource authenticated vlan を設定してください。

● IEEE802.1X認証が成功しない

【原因】 認証機能の使用定義で、システム定義またはポート定義の一方のみが設定されています。

【対処】 本装置の認証機能は、装置全体での使用定義（dot1x use、macauth use）と、認証を行うポートに対する使用定義（ether dot1x use、ether macauth use）によって動作します。
認証機能を利用する場合は、両方の定義で認証を有効に設定してください。

【原因】 ローカル認証でSupplicant側がEAP-MD5以外の認証アルゴリズムを指定しています。

【対処】 ローカル認証を利用する場合はEAP-MD5以外の認証アルゴリズムが利用できないため、Supplicant側の認証アルゴリズムの設定をEAP-MD5に変更してください。なお、最後の認証要求に関する情報はIEEE802.1X認証状態表示コマンド（show dot1x port）で確認できます。このコマンドの表示からSupplicant側で設定された認証アルゴリズムが判断できます。

【原因】 RADIUSサーバで登録された認証アルゴリズムと異なるアルゴリズムをSupplicantが要求しています。

【対処】 RADIUSサーバで登録された認証アルゴリズムとSupplicant側の認証アルゴリズムを同一のアルゴリズムにしてください。

● MACアドレス認証が成功しない

【原因】 RADIUSサーバの認証種別が誤っています。

【対処】 RADIUSサーバの認証種別（EITHER/CHAP/PAP）を、本装置の設定に合わせて設定してください。

● 認証が成功しているのに、Supplicantがネットワークへアクセスできない（共通）

【原因】 Supplicantに割り当てるVLAN IDが設定されていません。

【対処】 認証サーバ（RADIUSサーバまたはAAA設定）にSupplicantに割り当てるVLAN IDを設定してください。未設定の場合は、本装置のSupplicantに割り当てるデフォルトVLANの設定（ether dot1x vid、ether macauth vid）で定義されたVLAN IDが指定されたものとして動作します。

【原因】 Supplicantに割り当てるVLAN IDが誤っています。

【対処】 認証サーバ（RADIUSサーバまたはAAA設定）にSupplicantに割り当てるVLAN IDを設定してください。Supplicantに割り当てられたVLAN IDは、各認証の状態表示コマンド（show dot1x port、show macauth port）、または認証成功端末情報表示コマンド（show auth port）で確認できます。

2.8 SNMPに関するトラブル

SNMP機能でネットワークの管理を行う際のトラブルには、以下のようなものがあります。

● SNMPホストと通信ができない

【原因】 SNMPエージェントアドレスが正しく設定されていません。

【対処】 本装置のインタフェースに割り当てられているIPアドレスのどれかをSNMPエージェントアドレスとして設定してください。

【原因】 SNMPホストのIPアドレスが正しく設定されていません。

【対処】 本装置にアクセスするSNMPホストのIPアドレスを確認し、正しいIPアドレスを設定してください。

【原因】 コミュニティ名が正しく設定されていません（SNMPv1またはSNMPv2c使用時）。

【対処】 本装置にアクセスするSNMPホストのコミュニティ名を確認し、正しいコミュニティ名を設定してください。

【原因】 SNMPユーザ名が正しく設定されていません（SNMPv3使用時）。

【対処】 本装置にアクセスするSNMPホストのSNMPユーザ名を確認し、正しいSNMPユーザ名を設定してください。

【原因】 認証プロトコルまたは認証パスワードが正しく設定されていません（SNMPv3使用時）。

【対処】 本装置にアクセスするSNMPホストの認証プロトコルまたは認証パスワードを確認し、正しい認証プロトコルまたは認証パスワードを設定してください。

【原因】 暗号プロトコルまたは暗号パスワードが正しく設定されていません（SNMPv3使用時）。

【対処】 本装置にアクセスするSNMPホストの暗号プロトコルまたは暗号パスワードを確認し、正しい暗号プロトコルまたは暗号パスワードを設定してください。

2.9 VRRPに関するトラブル

VRRP機能を利用する際のトラブルには、以下のようなものがあります。

● VRRPグループが開始しない

【原因】 仮想IPアドレスが、装置に設定されたIPアドレスのどれかと同一です。

【対処】 仮想IPアドレスは、端末のIPアドレスのサブネットに一致し、装置に設定されたIPアドレスとは異なるIPアドレスを指定してください。

【原因】 装置内にVRIDが重複して設定されています。

【対処】 装置内でVRIDは一意である必要があります。異なるVRIDを設定してください。

● VRRPルータがマスタ状態となったのに通信不能となる

【原因】 仮想IPアドレスが、端末のIPアドレスのサブネットに一致するIPアドレスでありません。

【対処】 仮想IPアドレスを端末のIPアドレスのサブネットに一致するよう変更してください。

【原因】 仮想IPアドレスと同一のIPアドレスである装置が接続されています。

【対処】 仮想IPアドレスと同一のIPアドレスである装置のIPアドレスを変更してください。

【原因】 マスタ以外で、仮想IPアドレスを解決するARPリクエスト、またはNS（Neighbor Solicitation）メッセージに応答する装置が存在します。

【対処】 仮想IPアドレスを解決するARPリクエスト、またはNS（Neighbor Solicitation）メッセージに応答する装置の設定を応答しないように変更してください。

● プリエンプトモードoffに設定しても自動で切り戻る

【原因】 優先度が低い設定のVRRPルータにプリエンプトモードoffを指定しています。

【対処】 優先度が高い設定のVRRPルータにプリエンプトモードoffを指定してください。

【原因】 優先度に最優先（master）を指定しています。

【対処】 優先度に最優先（master）以外を指定してください。

【原因】 VRRPグループが開始してからプリエンプトモード移行禁止時間が経過していません。

【対処】 プリエンプトモード移行禁止時間中はプリエンプトモードonが指定されている場合と同じ動作となり、対処の必要はありません。

● 手動切り戻しできない

【原因】 マスタ状態のVRRPルータで手動切り戻しを実行しています。

【対処】 バックアップ状態（本来のマスタ）のVRRPルータで手動切り戻しを実行してください。

☛参照 コマンドユーザーズガイド「2.1.7 VRRP手動切り戻し機能を使う」（P.36）

【原因】 バックアップ状態ではあるが、現在の優先度が現在のマスタ状態のVRRPルータより低いです。

【対処】 バックアップ状態であるにもかかわらず切り戻らない場合は、VRRP情報を表示して現在の優先度、およびダウントリガ発動状態を確認してください。
ダウントリガが発動している場合は、ダウントリガが発動している原因を除去してください。
イニシャル状態である場合は、「● イニシャル状態から、バックアップ状態またはマスタ状態に遷移しない」（P.40）を参照してください。

【原因】 優先度が高い設定のVRRPルータにプリエンプトモードoffを指定していません。

【対処】 優先度が高い設定のVRRPルータにプリエンプトモードoffを指定してください。

● 本来のマスタが復旧したのに自動で切り戻らない

【原因】 プリエンプトモードがoffに設定されています。

【対処】 プリエンプトモードをonに設定してください。

【原因】 本来のマスタでダウントリガが発動しています。

【対処】 本来のマスタでVRRP情報を表示してダウントリガ発動状態を確認してください。
ダウントリガが発動している場合は、ダウントリガが発動している原因を除去してください。

● 単一VRRPグループに複数のマスタ状態であるVRRPルータが存在する

【原因】 VRRPグループである各VRRPルータのVRIDが同一でありません。
VRRP情報の「VRID illegal packets」がカウントされています。

【対処】 VRIDを同一の値に設定してください。

【原因】 VRRPグループである各VRRPルータのVRRPパスワード設定が同一でありません。
VRRP情報の「Authentication failed packets」または「Authentication type mismatch packets」がカウントされています。

【対処】 VRRPパスワード設定を同一にしてください。

【原因】 IPフィルタでVRRP-ADメッセージが遮断されています。

VRRP-ADメッセージ：

あて先IPアドレス　：224.0.0.18
ff02::12

プロトコル番号　　：112

IPv6 Next Header　：112

【対処】 VRRPルータのIPフィルタ設定でVRRP-ADメッセージが遮断される設定を削除してください。

【原因】 VRRPルータの接続方法が誤っています。

【対処】 VRRPルータを同一リンクに接続してください。

【原因】 VRRP情報の「TTL/HopLimit illegal packets」がカウントされています。

【対処】 VRRPルータを同一リンクに接続してください。

【原因】 VRRPルータを連結しているHUBでSTP機能を有効にしています。

【対処】 VRRPルータを連結しているHUBのSTP機能を無効に設定してください。

【原因】 VRRPルータを連結しているHUBの設定が誤っています。

【対処】 VRRPルータを連結しているHUBの設定を確認して、正しく設定し直してください。
VRRPルータどうしは同一リンクで接続される必要があります。
VRRPルータどうしはVRRP-ADメッセージを送受信可能である必要があります。

【原因】 VRRPルータを連結しているHUBが故障しています。

【対処】 VRRPルータを連結しているHUBを調べてください。

【原因】 本装置のSTP機能が有効です。

【対処】 本装置のSTP機能を無効にするか、VRRPグループを設定したインタフェースが使用するポート個別のSTP機能を無効にしてください。

● マスタが正常に切り替わったのに通信不能となる

【原因】 VRRP機能が有効であるlan設定でダイナミックルーティングを有効に設定しています。

【対処】 ダイナミックルーティングを無効に設定してください。

【原因】 端末のデフォルトルートが仮想IPになっていません。

【対処】 端末のデフォルトルートを仮想IPに設定してください。

【原因】 VRRPグループである各VRRPルータの仮想IPが同一でありません。
VRRP情報の「Virtual router IP address configuration mismatched packets」がカウントされています。

【対処】 仮想IPアドレスを同一に設定してください。

● 仮想IPアドレスあてのpingに応答しない

【原因】 仮想IPアドレスあてのicmp受信設定がされていません。

【対処】 仮想IPアドレスあてのicmp受信を有効に設定してください（lan vrrp group vaddr icmp accept）。

【原因】 仮想IPアドレスのVRRPグループがマスタ状態以外です。

【対処】 仮想IPアドレスあてのpingに応答するのは、マスタ状態のVRRPルータだけです。

● 仮想IPアドレスあてのtelnetが本装置につながらない

【原因】 VRRPが仮想IPアドレスあてのパケットが破棄されています。

【対処】 VRRPの仕様です。実IPアドレスをあて先に指定してください。

● マスタがバックアップになると実IPアドレスあての通信が不能となる

【原因】 優先度に最優先（master）を指定しています。

【対処】 優先度に最優先（master）以外を指定してください。

● ダウントリガが発動したのにマスタが切り替わらない

【原因】 優先度が低い設定のVRRPルータにプリエンプトモードoffを指定しています。

【調査方法】
プリエンプトモードをonに設定してください。
手動切り戻しとしたい場合は優先度が高い設定のVRRPルータにプリエンプトモードoffを指定してください。

【原因】 発動したダウントリガの優先度（優先度減算値）設定が小さい値を指定しています。

【対処】 （マスタの優先度値 - バックアップの優先度値）+1よりダウントリガの優先度を大きい値に設定してください。

【原因】 バックアップ側でダウントリガが発動しています。

【対処】 バックアップ側でVRRP情報を表示して現在の優先度、およびダウントリガ発動状態を確認してください。ダウントリガが発動している場合は、ダウントリガが発動している原因を除去してください。
必要に応じてマスタ側が発動したダウントリガの優先度設定を大きい値に変更してください。

● ノードダウントリガが一度発動すると復旧しない

【原因】 優先度に最優先（master）を指定しています。

【対処】 ダウントリガを使用する場合は優先度に最優先（master）を指定しないでください。

● ダウントリガの減算優先度の合計が255以上であるのにVRRP状態がイニシャル状態とならない

【原因】 ダウントリガが発動した場合、優先度の最低値は1以下にはなりません。

【対処】 本装置のVRRPの仕様です。VRRPの設定されたLANインタフェースに異常が発生するか、手動停止コマンドを実行しなければイニシャル状態とはなりません。

- **インタフェースダウントリガでPPPoEインタフェースを指定したが、異常が発生してもダウントリガが発動しない**

  【原因】 回線接続保持機能の設定が常時接続機能を使用するに指定されていません。

  【対処】 回線接続保持機能の設定を常時接続機能を使用するに指定してください。

- **リモート側もVRRPを構成して、ローカル側でマスタ切り替わりが発生すると通信不能となる**

  【原因】 ローカル側と対になるリモート側VRRPルータが同期して切り替わっていません。

  【対処】 同期して切り替わるようにダウントリガを設定してください。

- **イニシャル状態から、バックアップ状態またはマスタ状態に遷移しない**

  【原因】 VRRPグループ手動停止コマンドが実行されています（vrrp action disable）。

  【対処】 VRRPグループ手動再開始コマンドを実行してください（vrrp action enable）。
  手動停止コマンドが実行されているかは、VRRP情報を表示して確認することができます。現在のVRRPグループの状態がInitialize:Disabledの場合は手動停止コマンドが実行されています。

  【原因】 VRRPグループが設定されたLANで異常が発生しています。

  【対処】 LANケーブルの抜けや、接続されたHUBの異常などを確認してください。また、Etherに対して切断／閉塞コマンド（offline）が実行されていないかも確認してください。

- **VRRPアクションが一度発動すると復旧しない**

  【原因】 VRRPアクションでVRRPが設定されたLANに対して切断／閉塞コマンドが指定されています。

  【対処】 VRRPアクションでVRRPが設定されたLANに対して切断／閉塞コマンドが実行されないように設定してください。たとえば、切断／閉塞コマンドを実行する必要があるEtherを個別に指定します。

- **VRRPアクションの発動する状態にバックアップを指定したにもかかわらず、VRRPルータ開始時に発動しない**

  【原因】 VRRPアクションに切断／閉塞コマンドまたは接続／閉塞解除コマンドを指定しています。

  【対処】 VRRPアクションの切断／閉塞コマンドまたは接続／閉塞解除コマンドは発動する状態にバックアップを指定した場合、マスタ状態からマスタ状態以外に遷移しなければ発動しない仕様です。

- **VRRPアクションの発信抑止（diallock）または着信抑止（dialreject）が発動したのに発信抑止または着信抑止しない**

  【原因】 発信抑止または着信抑止するリモートがPPPoE接続以外です。

  【対処】 発信抑止または着信抑止の仕様です。

- **VRRPアクションの切断／閉塞コマンド（offline）が発動したのに対象が閉塞状態とならない**

  【原因】 切断／閉塞する対象がPPPoE接続またはテンプレート着信による接続となっています。

  【対処】 切断／閉塞コマンドの仕様です。

2.10 外部メディアスタート機能に関するトラブル

外部メディアスタート機能に関するトラブルには、以下のようなものがあります。

- **USB メモリを取り付けした USB ポートのランプが橙色で点灯している。**

【原因】 外部メディアスタート機能が異常終了しました。

【対処】 システムログメッセージまたは USB メモリ内に作成された「output.txt」の内容を参照し、エラー内容を確認してください。

【原因】 外部メディアスタート機能でパスワード認証エラーが発生しました。

【対処】 装置に管理者パスワードが設定されている場合は、パスワードファイルを USB メモリ上に用意する必要があります。

参照 コマンドユーザーズガイド「2.7.3 パスワードファイルの作り方」（P.54）

- **装置が起動できない**

【原因】 外部メディアスタート機能の動作中に USB メモリが抜けた、または本装置の電源ケーブルが抜かれたなどの理由で、ソフトウェアのインストールに失敗した可能性があります。

【対処】 バックアップファームを起動し、ソフトウェアをインストールしてください。

参照 Si-R G200　ご利用にあたって
「3.5 ソフトウェア更新に失敗したときには（バックアップファーム機能）」（P.73）
Si-R G100　ご利用にあたって
「3.5 ソフトウェア更新に失敗したときには（バックアップファーム機能）」（P.61）

2.11 その他のトラブル

その他、以下のようなトラブルがあります。

- **データ通信はほとんどしていないはずなのに、通信料金が高い**

【対処】
- システムログを確認してください。
- Windows（TCP 上の NetBIOS）環境のネットワークでは、セキュリティ上の問題と、超過課金を抑えるために、ポート番号 137～139 の外向きの転送経路をふさいでおく必要があります。必要に応じて IP フィルタリングを正しく設定してください。

3 コマンド入力が正しくできないときには

コマンドで設定や操作を行ったときに正しくコマンドが入力できない場合は、まず、以下を参考に本装置の動作状況を確認してみてください。

3.1 シェルに関するトラブル

シェルで入力編集を行う際のトラブルには、以下のようなものがあります。

- **シェルでの入力編集やページャ表示時に、カーソルが変な位置に移動してしまう**

【原因】 端末の画面サイズが正しく設定されていません。

【対処】 terminal window コマンドで正しい画面サイズを設定し直してください。

【原因】 画面サイズを通知しないtelnet クライアントを使用しています。

【対処】 画面サイズを通知するtelnetクライアントを使用してください。または、terminal windowコマンドで正しい画面サイズを設定し直してください。

- **特定の［Ctrl］+［α］キーが動作しない（［α］キー：任意のキー）**

【原因】 端末ソフトウェアが［Ctrl］+［α］キーを処理してしまうため入力できません。

【対処】 端末ソフトウェアの設定で、［Ctrl］+［α］キーを使用できるよう設定してください。
端末ソフトウェアに［ESC］キー（次に入力したキーをそのまま入力するキー）が用意されているのであれば、［ESC］キーを入力したあと［Ctrl］+［α］キーを入力してください。

- **矢印キー（↑、↓、←、→）が動作しない**

【原因】 矢印キーをサポートしていない端末ソフトウェア（HyperTerminalなど）を使用しています。

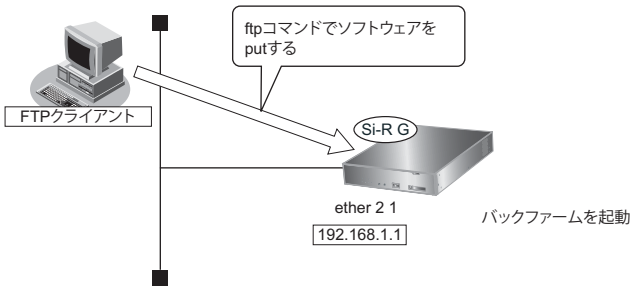
【対処】 矢印キーの代わりに［Ctrl］+［B］キーおよび［Ctrl］+［F］キーでカーソル移動、［Ctrl］+［P］キーおよび［Ctrl］+［N］キーでコマンド履歴移動を行ってください。

4 ソフトウェア更新に失敗したときには（バックアップファーム機能）

停電などでソフトウェアの更新に失敗し、本装置を起動できなくなった場合、バックアップ用のファームを起動し、ネットワーク上のFTPクライアントからソフトウェアを転送することにより、正常な状態に復旧することができます。

補足 リセットスイッチを押しながら電源を投入するとバックアップファームが起動されます。

ここでは、Si-R G200を例に説明します。



4.1 パソコン（FTPクライアント）を準備する

1. 更新するためのソフトウェアをFTPクライアントに保存します。

4.2 本装置を準備する

こんな事に気をつけて

バックアップファームが起動した場合、本装置のetherグループ2ポート1のIPアドレスは192.168.1.1になっています。運用中のLANで、このアドレスに問題がある場合は、FTPクライアントだけを接続してください。

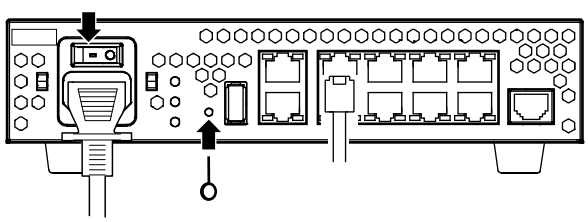
1. 本装置の電源が切れていることを確認します。

2. 本装置とパソコン（FTPクライアント）をLAN接続します。

本装置とパソコンをHUBを介さず、直接、10/100/1000BASE-Tポートにケーブルを接続します。

補足
- ツイストペアケーブルを機器に接続する直前に、静電気除去ツールなどを使用してケーブルに帯電している静電気を除電してください。除電については、以下を参照してください。
  Si-R G200　ご利用にあたって「ツイストペアケーブルの除電について」（P.11）
  Si-R G100　ご利用にあたって「ツイストペアケーブルの除電について」（P.11）
- 本装置は、AutoMDI/MDI-X機能をサポートしているため、パソコンとHUBを意識しないで、10/100/1000BASE-Tポートにケーブルを接続することができます。

3. 先の細いものでリセットスイッチを押しながら電源を投入します。



4.　約5秒後にリセットスイッチをはなします。

バックアップファームが起動します。

こんな事に気をつけて

電源投入後、10秒以内にリセットスイッチをはなさない場合、リセットスイッチの故障とみなされます。
そのため、約5秒後に必ずリセットスイッチをはなしてください。

補足
- バックアップファームの起動には約1分かかります。
- バックアップファームが動作しているときは、CHECKランプが緑色で点灯します。

4.3　ソフトウェアを更新する

1.　パソコン（FTPクライアント）から本装置にソフトウェアを転送します。

参照 コマンドユーザーズガイド「2.5.2 FTPサーバ機能によるソフトウェアの退避／更新」（P.45）

こんな事に気をつけて

- **ソフトウェアの転送（put）中は、本装置の電源を切断しないでください。**
- **転送中に電源を切断すると、本装置が使用できなくなる場合があります。**

2.　ソフトウェアの更新が正常に行われたことをランプで確認し、電源を切断します。

補足 ソフトウェア更新中はCHECKランプが緑色で点滅し、更新が完了後、CHECKランプの緑色点滅は終了します。

3.　電源を投入すると、更新したソフトウェアで本装置が起動します。

5　ご購入時の状態に戻すには

本装置を誤って設定した場合やトラブルが発生した場合、コンソールケーブルやLANケーブル、またはSELECTボタン／ENTERボタンを使用することで、本装置をご購入時の状態に戻すことができます。
また、本装置を移設する場合は、ご購入時の状態に戻してから設定してください。

こんな事に気をつけて

ご購入時の状態に戻すと、それまでの設定内容がすべて失われます。構成定義情報の退避、または設定内容をメモしておきましょう。

用意するもの（「5.3 SELECTボタン／ENTERボタンを使用する」（P.49）の場合は不要）

- コンソールケーブルまたはLANケーブル

補足　本製品には、コンソールケーブルは同梱されていません。
「5.2 コンソールポートに接続する」（P.47）の方法でご購入時の状態に戻す場合は、コンソールケーブルを用意してください。
ケーブルについては、以下の富士通ホームページをご覧ください。
URL : http://fenics.fujitsu.com/products/manual/cable3/

参照　仕様一覧「1.2 コンソールポート仕様」（P.11）

- ターミナルソフトウェア（HyperTerminalなど）

ここでは、Si-R G200を例に説明します。

5.1　LANで接続する

本装置を準備する

こんな事に気をつけて

バックアップファームが起動した場合、本装置のetherグループ2ポート1のIPアドレスは192.168.1.1になっています。運用中のLANで、このアドレスに問題がある場合は、パソコンだけを接続してください。

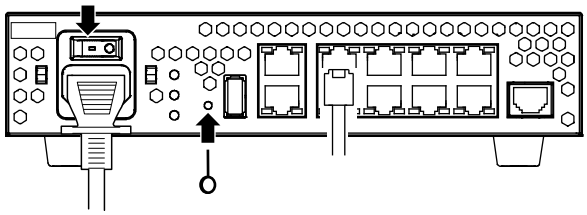
1.　本装置の電源が切れていることを確認します。

2.　本装置とパソコンをLAN接続します。

本装置とパソコンをHUBを介さず、直接、10/100/1000BASE-Tポートにケーブルを接続します。

補足
- ツイストペアケーブルを機器に接続する直前に、静電気除去ツールなどを使用してケーブルに帯電している静電気を除電してください。除電については、以下を参照してください。
  Si-R G200　ご利用にあたって「 ツイストペアケーブルの除電について」（P.11）
  Si-R G100　ご利用にあたって「 ツイストペアケーブルの除電について」（P.11）
- LANケーブルの接続方法およびパソコンの準備については、以下を参照してください。
  Si-R G200　ご利用にあたって「2.5 設定用パソコンを接続する」（P.40）
  Si-R G100　ご利用にあたって「2.4 設定用パソコンを接続する」（P.30）
- 本装置は、AutoMDI/MDI-X機能をサポートしているため、パソコンとHUBを意識しないで、10/100/1000BASE-Tポートにケーブルを接続することができます。

3.　先の細いものでリセットスイッチを押しながら電源を投入します。



4.　約5秒後にリセットスイッチをはなします。

バックアップファームが起動します。

こんな事に気をつけて

電源投入後、10秒以内にリセットスイッチをはなさない場合、リセットスイッチの故障とみなされます。
そのため、約5秒後に必ずリセットスイッチをはなしてください。

補足
- バックアップファームの起動には約1分かかります。
- バックアップファームが動作しているときは、CHECKランプが緑色で点灯します。

本装置をご購入時の状態に戻す

1.　telnetでログインします。

パソコンには、本装置と同じネットワークのIPアドレスを設定してください。本装置のご購入時のIPアドレスは「192.168.1.1」、サブネットマスクは「255.255.255.0」です。

2.　[Return]キーまたは[Enter]キーを押します。

3.　画面に「backup#」と表示されたことを確認します。

4.　reset clearと入力して、[Return]キーまたは[Enter]キーを押します。

本装置の構成定義情報が初期化されます。

```
backup# reset clear（下線部入力）
```

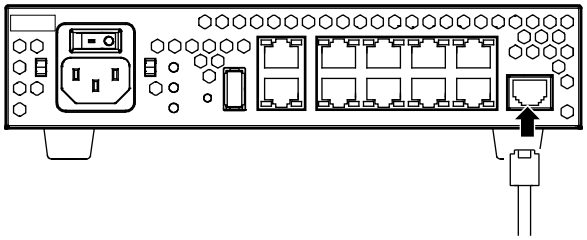
5.　CHECKランプが緑色で点灯状態になったことを確認したあとに電源を再投入します。

本装置がご購入時の状態で起動します。

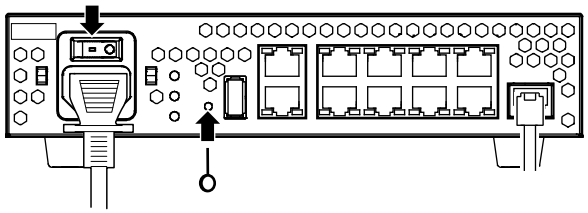
5.2　コンソールポートに接続する

本装置を準備する

1. 本装置の電源が切れていることを確認します。
2. パソコンとコンソールケーブルを接続します。
3. 本装置のコンソールポートにコンソールケーブルのRJ45プラグを差し込みます。



4. 先の細いものでリセットスイッチを押しながら電源を投入します。



5. 約5秒後にリセットスイッチをはなします。

   バックアップファームが起動します。

こんな事に気をつけて

電源投入後、10秒以内にリセットスイッチをはなさない場合、リセットスイッチの故障とみなされます。
そのため、約5秒後に必ずリセットスイッチをはなしてください。

補足
- バックアップファームの起動には約1分かかります。
- バックアップファームが動作しているときは、CHECKランプが緑色で点灯します。

本装置をご購入時の状態に戻す

1. **パソコンでターミナルソフトウェアを起動します。**
2. **設定条件を以下のように設定します。**

スタートBit	データBit	パリティ Bit	ストップBit	同期方式	通信速度	フロー制御
1	8	なし	1	非同期	9600	なし

補足 設定条件の設定方法については、ターミナルソフトウェアのマニュアルを参照してください。

3. **［Return］キーまたは［Enter］キーを押します。**
4. **画面に「>」と表示されたことを確認します。**
5. **logonと入力して、［Return］キーまたは［Enter］キーを押します。**
6. **画面に「backup#」と表示されたことを確認します。**
7. **reset clearと入力して、［Return］キーまたは［Enter］キーを押します。**

   本装置の構成定義情報が初期化されます。

```
>logon
backup# reset clear（下線部入力）
>
```

8. **CHECKランプが緑色で点灯状態になったことを確認したあとに電源を再投入します。**

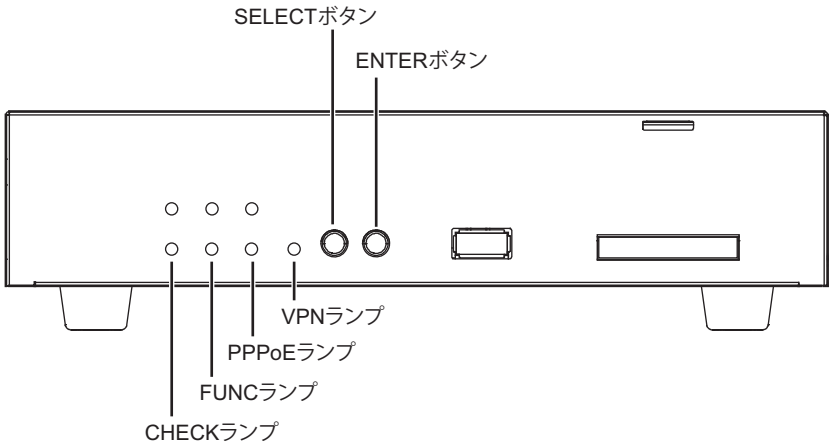
   本装置がご購入時の状態で起動します。

5.3 SELECTボタン／ENTERボタンを使用する

⚠注意

LANケーブルや通信モジュールを取り外してから本操作を実行してください。
ソフトウェア更新中などに本操作を行った場合、本装置を起動できなくなったり、正常に実行されない場合があります。

本装置をご購入時の状態に戻す



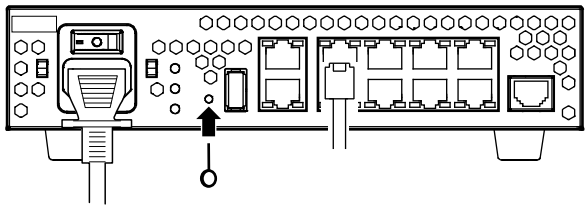
1. **本装置の電源を投入し、装置が起動したことを確認します。**
   本装置前面のPOWERランプが緑色で点滅後、点灯します。

2. **SELECTボタンを1回押します。**
   PPPoEランプが消灯し、VPNランプが緑色で点滅したことを確認します。

3. **SELECTボタンをさらにもう1回押します。**
   VPNランプが消灯し、PPPoEランプが緑色で点滅したことを確認します。

4. **ENTERボタンを押します。**
   PPPoEランプが緑色／橙色で交互に点滅したことを確認します。

5. **先の細いものでリセットスイッチを押します。**
   本装置の構成定義情報が初期化され、本装置がご購入時の状態で起動します。



こんな事に気をつけて

手順2.～4.で、次の手順が10秒以上行われない場合、元の状態に戻ります。
再度手順2.から行ってください。

索引

C

CHECK ランプ 11

F

FTP クライアント 43

H

HyperTerminal 45

I

ipconfig 13

L

LAN ケーブル 45

N

NetBIOS 41

P

POWER ランプ 11
PPPoE 接続 16

R

RIP パケット 7

S

SELECT ボタン 49

T

telnet 13

W

Windows NT 4.0 14

え

エラーログ情報 11

か

回線料金 7

こ

購入時の状態に戻す 45
コンソールケーブル 45

し

自動送信パケット 8

す

スケジュール機能 9

そ

ソフトウェア更新 44

た

ターミナルソフトウェア 45

ち

超過課金 7

つ

通信料金 41

て

データ通信 15
デフォルトルート 9

は

パスワード 13
バックアップファーム機能 43

ほ

本装置 IP アドレス 13

ま

マニュアル構成 6

り

リセットスイッチ 47

Si-R Gシリーズ　トラブルシューティング

P3NK-4472-08Z0

発行日　　2014年11月

発行責任　　富士通株式会社

• 本書の一部または全部を無断で他に転載しないよう、お願いいたします。
• 本書は、改善のために予告なしに変更することがあります。
• 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、 弊社はその責を負いません。